

McDonald Hopkins

A business advisory and advocacy law firm®

James J. Giszczak
Direct Dial: 248.220.1354
E-mail: jgiszczak@mcdonaldhopkins.com

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

May 13, 2016

RECEIVED

MAY 17 2016

ATTORNEY GENERAL OF INDIANA
CONSUMER PROTECTION

Ms. Stephanie Kindred
Consumer Protection Division
Identity Theft Unit
Office of the Indiana Attorney General
302 W. Washington Street, 5th Floor
Indianapolis, IN 46204-2770

Re: Wood Herron & Evans, LLP – Incident Notification

Dear Ms. Kindred:

McDonald Hopkins PLC represents Wood Herron & Evans (“WHE”). I write to provide notification concerning a privacy incident that may affect the security of personal information of two (2) Indiana residents. WHE’s investigation has concluded and this notification is being provided voluntarily. By providing this notice, WHE does not waive any rights or defenses regarding the applicability of Indiana law or personal jurisdiction.

WHE uses a third party vendor to provide payroll services for its employees. On April 11, 2016 WHE was notified that an unauthorized user accessed WHE employee information on April 10 and 11 through the vendor portal that stores payroll information. The unauthorized third party attempted to, or did, change direct deposit information of some employees on April 11 before the access was discovered. Fortunately, the files that were accessed were limited only to payroll information and only a small number of employees’ information was accessed. No security codes, passwords or access codes for the bank accounts were accessible.

After being notified of this issue, WHE immediately notified all of its employees on April 11, 2016, (see attached) commenced an investigation and engaged external cybersecurity professionals who regularly investigate and analyze these types of incidents to determine the extent of the compromise and assist in its response. WHE also made certain that the system was secure and the unauthorized access had been terminated.

Based on WHE’s complex forensic investigation which was concluded on May 3, 2016, WHE can confirm that payroll information, including direct deposit information, including bank account number and routing information may have been accessed by the unauthorized third party. However, no security codes, passwords or access codes for the bank accounts were accessible. Moreover, no other personal or medical information was accessible within the compromised account. Specifically, Social Security numbers and other personally identifiable

Ms. Stephanie Kindred
Consumer Protection Division
Identity Theft Unit
Office of the Indiana Attorney General
May 13, 2016
Page 2

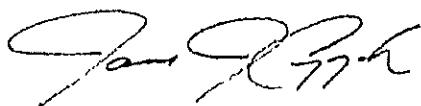
information **were not** in the compromised account, and therefore, were not accessible or accessed.

To date, WHE is not aware of any reports of identity fraud as a direct result of this incident. Nevertheless, we wanted to make you (and the affected residents) aware of the incident and explain the steps WHE is taking to safeguard the residents against identity fraud. WHE provided the Indiana residents with written notice of this incident commencing on April 11, 2016 and again on April 15 and 21, 2016, as well as May 9 (see attached). WHE also provided notice to the residents on May 11, 2016, in substantially the same form as the letter attached hereto. WHE has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. WHE is also offering the residents a complimentary one-year membership with a credit monitoring and identity theft restoration service and is answering any questions directly. WHE has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

WHE is committed to maintaining the privacy of personal information and has taken many precautions to safeguard it. WHE continually evaluates and modifies its practices to enhance the security and privacy of personal information, which includes training its workforce on security threats.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,



James J. Giszczak

JJG/kjb
Encl.